Building a Secure and Survivable Next Generation Internet

Marilyn McAllister
SY Technology, Huntsville AL
A Division of L3 Communications
Marilynm@sy.com
256-704-9627

Agenda

- Architectural Weaknesses of Today's Internet
- Network and Network Security Architectures of the Future (2005+)
- Technologies Needed to Address Weaknesses
- Issues

Architectural Weaknesses of Today's Internet

Physical Architecture:

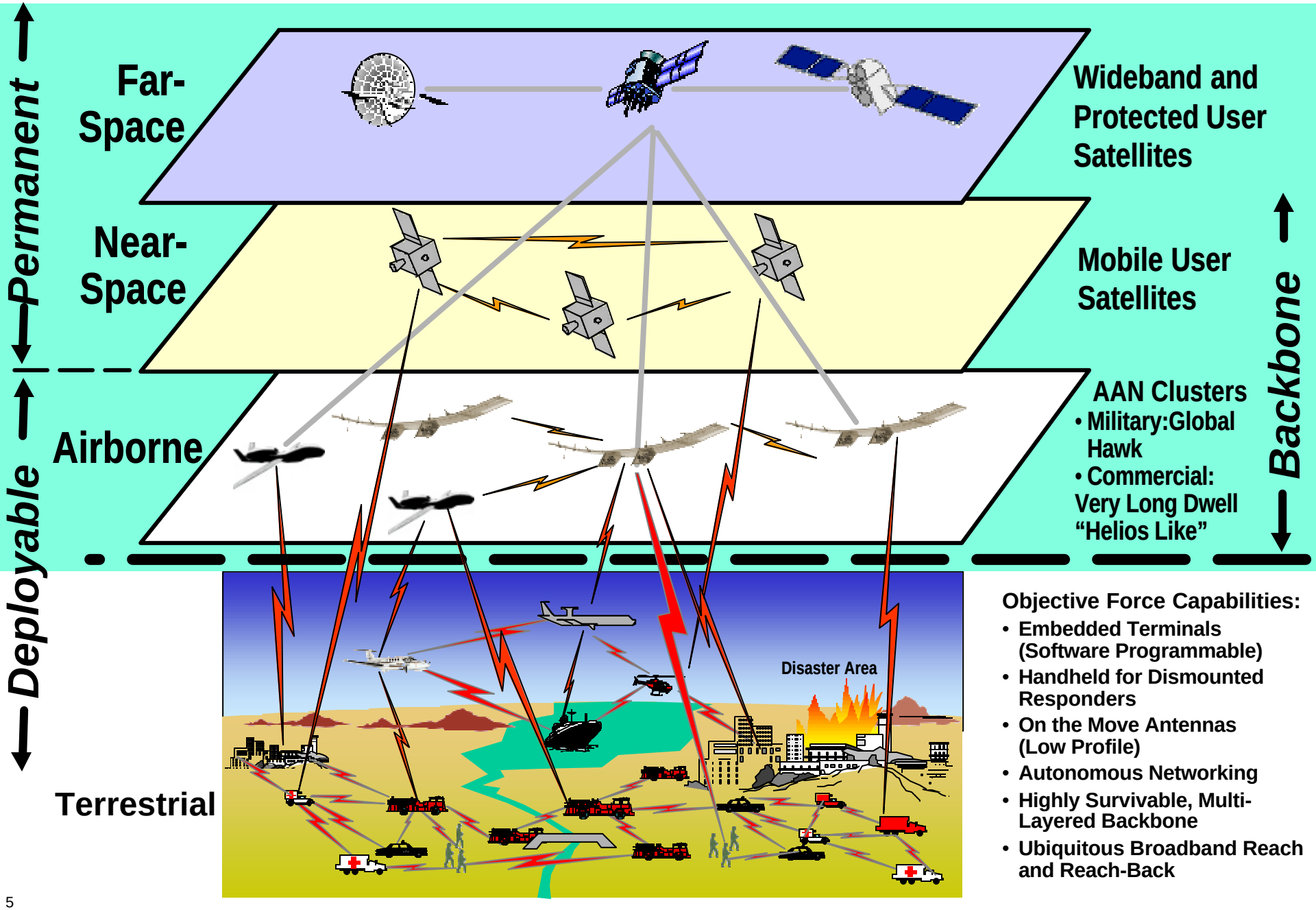
- Single layer Terrestrial Architecture heavily reliant on fiber backbone.
  - Easy to attack (backhoe, shovel, fishing net, boat anchor, bomb)
  - Fiber route locations available in the public domain
  - Repair/restoration time consuming
  - Extended regional outages possible

Architectural Weaknesses of Today's Internet

Network Security Architecture Weaknesses :

- Security Architectures Developed as afterthought
- Thousands of "back doors" and vulnerabilities
- Application of "software patches" time consuming
- The technical skills to identify and properly respond to major cyber attack beyond the skills of most systems administrators or network managers
- Tools to identify and respond to attacks inadequate
  - Just identifying whether the problem is an attack or system failure often difficult
- New "exploits" discovered and published worldwide daily
- Attacks becoming more sophisticated, software scripts widely available, required skills to conduct attack decreasing
- A risk accepted by one in the network is a risk imposed on all

Survivable Network Architecture (Homeland Security Response Force 2010+)



Objective Force Capabilities:

- Embedded Terminals (Software Programmable)
- Handheld for Dismounted Responders
- On the Move Antennas (Low Profile)
- Autonomous Networking
- Highly Survivable, Multi-Layered Backbone
- Ubiquitous Broadband Reach and Reach-Back

Building a Secure And Survivable Internet: Future Technologies to Enhance Physical Survivability

(Internet in Space Adds Survivable Layer to Internet Architecture)

- **Space:**
  - **Laser and Broadband Radio Frequency Cross-Links**
  - **Optical Switching**
  - **Cross-banding**
  - **On Board Switching and Routing**

(Provides Emergency Restoration if Terrestrial Infrastructure Damaged or Destroyed)

- **Air:**
  - **Long Loiter High Altitude Unmanned Vehicles**
  - **Broadband Communications Links (To Space, Air, Terrestrial)**
  - **On Board Switching And Routing**

(Reduces Reliance on Vulnerable Fiber Links, Speeds Restoration)

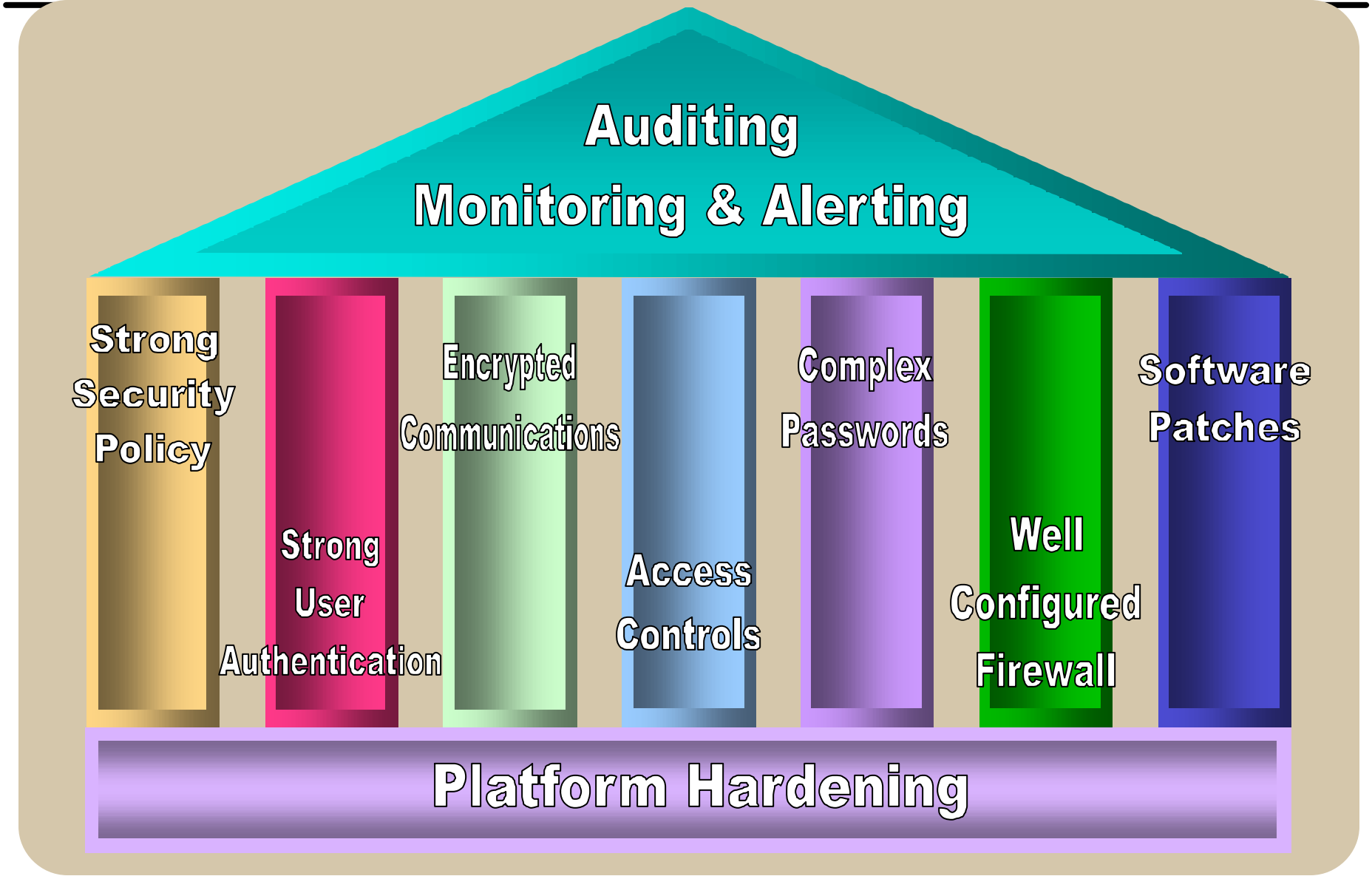
- **Terrestrial**
  - **Broad Band Radio Frequency Nodes and User Terminals**
  - **Directional Antennas (Phased Array)**
  - **Rapid Recovery Nodes/Teams**

Building a Secure And Survivable Internet: Future Technologies to Enhance Physical Survivability

(Assures Rapid Restoration and Enhances Security)

- **Network:**
  - **Autonomous Networking**
  - **Ad Hoc Networking Protocols**
  - **Secure “Next Generation IP”**

Network Security Architecture



Building a Secure And Survivable Internet: Future Technologies to Enhance Cyber Security

- Broadband Radio Frequency and Laser Link Encryption
- Unbreakable End to End Encryption (Quantum?)
- Advanced Firewalls
- Real Time Attack Sensing (vs. System Failure)
- Advanced Intrusion Detection
- Attacker Response: Hot Pursuit, Backtracking, Disabling
- Network and Computer Forensics
- Trojan Horse Detectors
- Advanced Virus Detectors
- Virus “Sponge”
- Advanced System “Scrubbers”and “Sanitizers”
- Advanced Software Patch Implementation
- Advanced Network Security Scanning
- “Virtual Presence” Network Security Monitoring

Secure And Survivable Internet

Architectural Design Principles

Physical Security Enhancements:

- Multi-Layered Network Architecture (Space, Air, Terrestrial Layers)
- Redundant Nodes, Multi-Link Topologies (Eliminate Single Point Failures)

Cyber Security Enhancements:

- Multi-Layered Network Security Architecture
- Security Standards Compliance (ISO 17799, etc.)

Both:

- Systems And Network Hardening
- Back Door Elimination

Building a Secure And Survivable Internet: Information Infrastructure Protection Issues

- **Who Is The Overall Integrator?**
  - Government + Commercial, Space+ Air+Terrestrial
  - Who Pays?
- **What Is The Role Of The Department Of Homeland Security?**
- **Are DoD "Protected" and/or "Secure" Communications Needed to Support Mission Critical Commercial Users In Homeland Security Scenarios?**
  - (Banking, Commerce, Transportation, Medical, etc.)
- **How Much "Protected" Communications Are Required To Run Federal, State, Local Governments, Restore Critical Economic Functions, And Support Disaster Recovery Teams?**
- **Who Gets Communications Priority?**
- **Is A System Similar to DoD's INFOCON Levels Needed For the U.S. Commercial Internet Based On Cyber Threat Level?**
  - Are there scenarios where the U.S. commercial Internet would be shut off from the rest of the world to protect our infrastructure from attack.
  - How do we respond to attacks originated in other countries?


WE'RE NOT INTERESTED.
FIREWALL
INTRUSION DETECTION SIDING
GSA
©01 Hlasner FCW